IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

IN THE MATTER OF THE SEARCH OF **4206 FM667, FROST, NAVARRO COUNTY, TEXAS 76441**	Case No. 24-mj-2294 **Filed Under Seal**

MOTION TO SEAL SEARCH WARRANT AND ALL RELATED DOCUMENTS

The United States of America, by and through Henry C. Leventis, United States Attorney for the Middle District of Tennessee, and Joshua A. Kurtzman, Assistant United States Attorney, hereby moves this Court to seal the search warrant and all related documents in the above-referenced case in order to protect the ongoing investigation. However, the Government requests that it be allowed to disclose such sealed documents to counsel for any defendant in the above-referenced case, or any related case, in order to comply with its discovery obligations under Federal Rule of Criminal Procedure 16 and its *Brady/Giglio* obligations. And, the Government requests the right to redact the search warrant and all related documents in order to protect potential witnesses and/or personal identifying information.

Executed on September 20, 2024.

//s// *Joshua A. Kurtzman*
JOSHUA A. KURTZMAN
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

IN THE MATTER OF THE SEARCH OF **4206 FM667, FROST, NAVARRO COUNTY, TEXAS 76441**	Case No. 24-mj-2294 **Filed Under Seal**

ORDER SEALING SEARCH WARRANT AND ALL RELATED DOCUMENTS

This matter comes before the Court on the United States' Motion to Seal the Search Warrant and All Related Documents. The motion is GRANTED and it is hereby ordered that:

The search warrant and all related documents be sealed, pending further order of the Court. The Government may disclose such sealed documents to counsel for any defendant in the above-referenced case, or any related case, in order to comply with its discovery obligations under Federal Rule of Criminal Procedure 16 and its *Brady/Giglio* obligations. The Government also reserves the right to redact the search warrant and all related documents in order to protect potential witnesses and/or personal identifying information.

September 20, 2024
Date

JEFFERY S. FRENSLEY
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the

Middle District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4206 FM667, FROST, NAVARRO COUNTY, TEXAS 76441

Case No. 24-mj-2294

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 875(c)	communicating a threat in interstate commerce

The application is based on these facts:

See attached statement

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Angelo DeFeo
Applicant's signature

FBI SA Angelo DeFeo
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: September 20. 2024

Judge's signature

City and state: Nashville, Tennessee

Jeffery S. Frensley, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF: **4206 FM667, FROST, NAVARRO COUNTY, TEXAS 76441**	No. 24-mj-2294

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Angelo DeFeo, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 4206 FM667, FROST, NAVARRO COUNTY, TEXAS, hereinafter "PREMISES," located within the Northern District of Texas, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and have been since February of 2016. I am currently assigned to the Memphis Field Office – Nashville Resident Agency. In my duties as an FBI Special Agent, I have received training in and have experienced with investigating violent crimes, including participating in surveillance, investigative interviews, and the execution of search and arrest warrants. As a federal agent, I am authorized to investigate violations of laws of the United States, and as a law enforcement officer I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all of my knowledge, or the knowledge of others, about this matter.

4. Rule 41 of the Federal Rules of Criminal Procedure provides that "a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district." Fed. R. Crim. P. 41(b)(3).[1]

5. Title 18, United States Code, Section 2331(5) defines the term "domestic terrorism" as activities that occur primarily within the territorial jurisdiction of the United States that appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

6. As an agent, the focus of my work is on domestic terrorism and other violent crime. The FBI has categorized this investigation as one involving domestic terrorism. Moreover, activities related to the domestic terrorism under investigation have occurred within the Middle District of Tennessee.

7. Based on my training and experience and the facts as set forth in this affidavit, I respectfully submit that there is probable cause to believe that violations of 18 U.S.C. § 875(c) (threatening interstate communications) (the "Target Offense") have been committed by David Aaron BLOYED ("the Subject") and other identified and unidentified persons, including others who may have been aided and abetted by, or conspired with, the Subject, as well as others observed by the Subject. There is also probable cause to search the PREMISES including any persons at or associated with this residence and any vehicles located at or near the premises that fall under the

[1] The United States has disclosed to the Court that a previous warrant was issued for this property in the Northern District of Texas in Case Number 3:24-MJ-868-BK. The United States is resubmitting this warrant to provide greater fidelity as to the property to be searched.

dominion and control of the persons associated with said premises and any digital devices, further described in Attachment A, for the things described in Attachment B.

PROBABLE CAUSE

Background

8. Goyim Defense League (GDL) is a small network of antisemitic provocateurs who espouse vitriolic antisemitism via the internet, through propaganda distributions and in street actions.

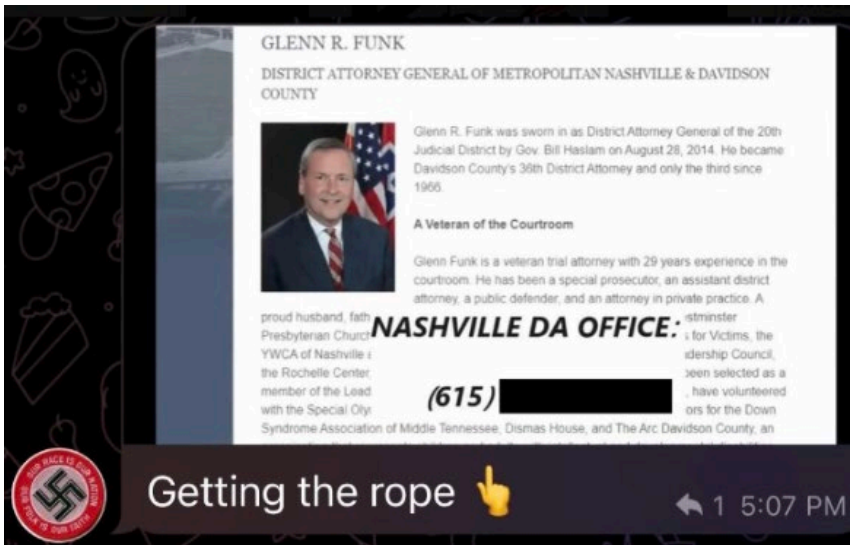
9. GDL organizes what it calls the "Name the Nose Tour" where its members travel to cities across the country to protest in the vicinity of synagogues and walk through the downtown hubs of the cities they are in with Nazi flags and yell antisemitic slurs at any individuals they encounter.

10. According to public reporting, GDL engages in mailing antisemitic postcards, public banner drops, protesting outside of synagogues for, and participating in what it calls a "City Council Death Squad (CCDS)." A CCDS is when GDL members engage in disruptive behavior and antisemitic speech at public forums such as city councils, county boards, and state house committee meetings. During stops on the "Name the Nose Tour," GDL members have been known to engage in violent activity that has led its members to be arrested by local, state, and federal law enforcement for threatening communications, aggravated assault, battery, and illegally carrying firearms.

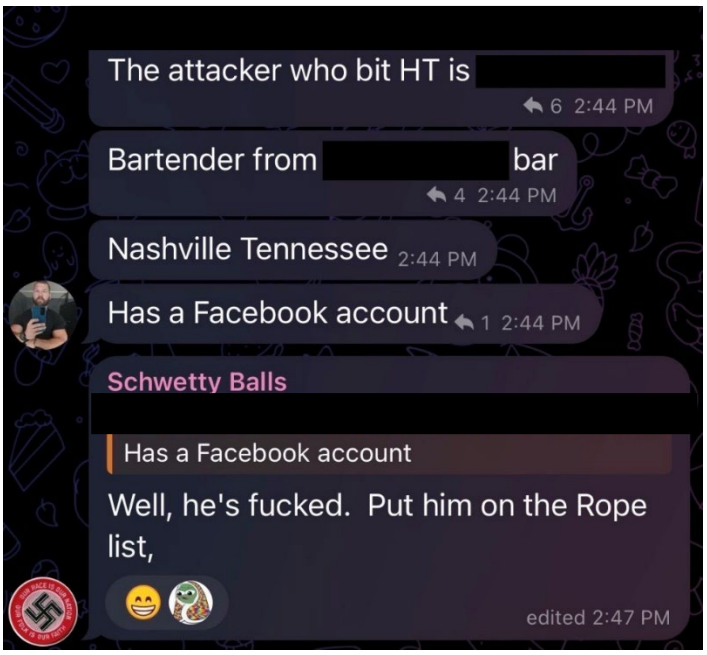
11. In July 2024, members of GDL were present in the Nashville area as part of their "Name the Nose Tour 6." On or about July 14, 2024, members of GDL were protesting downtown Nashville when certain participants in the protest encountered an employee of one of the local establishments. A physical altercation occurred, and as a result, an individual known to be a GDL

member, GDL member 1, was arrested and charged with Aggravated Assault due to his hitting the bar employee repeatedly with a metal flagpole that had a flag with a swastika affixed to the top of it.

12. During GDL's presence in Nashville, individuals who identify with GDL were routinely posting about their activities on various social media platforms, to include Telegram. Open-source research revealed that following the arrest of a GDL member 1, Telegram username "Schwetty Balls" posted the following threat against Davidson County District Attorney("DA") Glenn Funk:



13. In addition to threatening DA Funk, Telegram username "Schwetty Balls" also posted the following threat to the victim of the Aggravated Assault that occurred on or about July 14, 2024:



Identification of David Aaron BLOYED

14. Following the threats made by "Shwetty Balls" on Telegram, law enforcement conducted open-source research which revealed a Gab account with an almost identical username, "Shwettyballs." Gab, like Telegram, is a social media site.

15. On or about August 9, 2024, a subpoena was served to Gab for subscriber information. The results of the subpoena outlined that the Gab account that made the threat to DA Funk and others belonged to a user who registered for the account with email address is subscribed to email address dbloyed@airmail.net. A review of a law enforcement database revealed that dbloyed@airmail.net is an email account registered to BLOYED.

16. A review of the subpoena return registered to dbloyed@airmail.net identified that that the user identified as a "Nat Soc," which is understood to mean that the user is a national socialist or neo-Nazi, and the user also identified himself as "White Aryan not jewish." The user also identified his enemies in the following account header in a manner that is consistent with the beliefs of GDL: "My enemies are: jews, Royals, judeo church faggots, secret societies, all of them. Its the jews!"

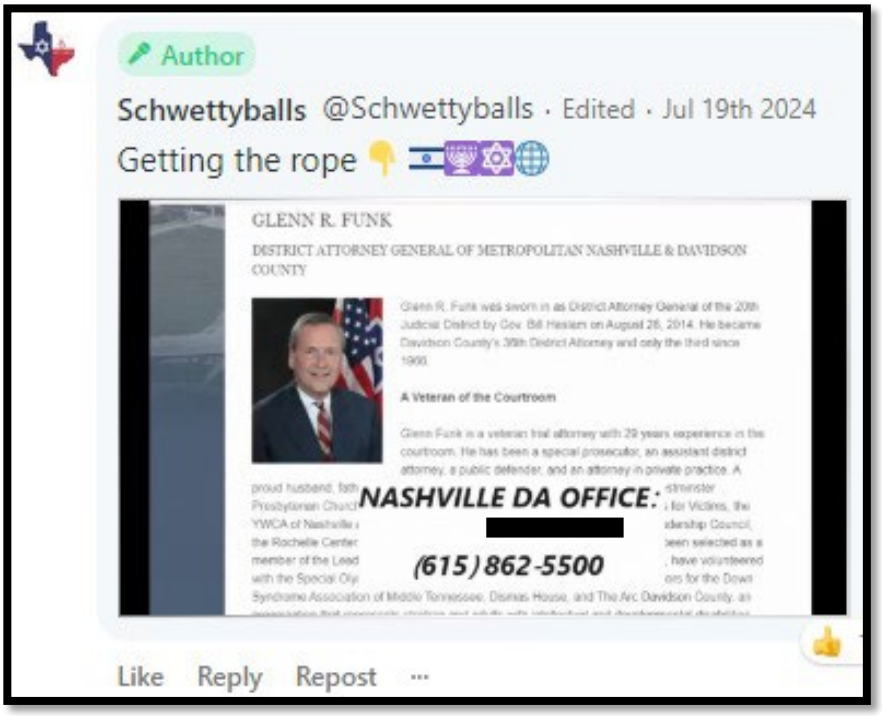
17. On or about August 26, 2024, a subpoena was served to AMA TechTel for the subscriber information related to the IP address that was utilized to create the Gab account "Schwettyballs." The results of the subpoena revealed the address in which the IP address originated was 4206 FM 667, Frost, Texas 76641. A property records search revealed this address is owned by David Aaron BLOYED.

18. On or about August 26, 2024, a subpoena was served to AT&T for the subscriber information related to phone number 972-567-6523. The results of the subpoena revealed the phone number was subscribed to David BLOYED. Additionally, the home contact email address

for the AT&T account was "Dbloyed@airmail.net," which is the same email address used to register the "Schwettyballs" Gab account.

19. BLOYED, the user of this Gab account, closely followed the GDL's activities in Nashville that included liking a post that stated "FREE RYAN KRIEGER" that also had a link to a fundraising site seeking donations to aid GDL member 1.

20. A review of BLOYED's Gab account revealed a Texas-themed profile photograph on BLOYED's Gab account. A review of BLOYED's Gab account revealed nearly identical threatening posts as BLOYED's Telegram account, as detailed below:

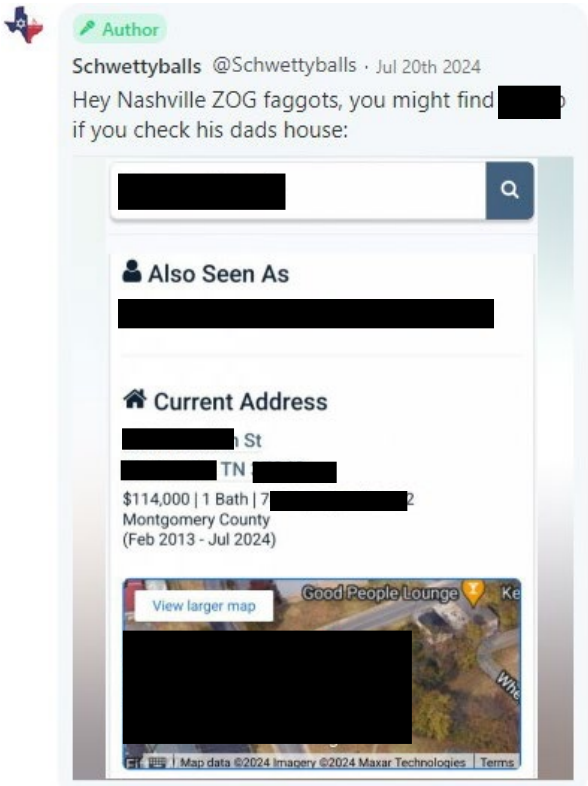


21. The above post from BLOYED's Gab account displayed the exact same post that was made by BLOYED on Telegram on or about July 14, 2024.

22. BLOYED also commented on GDL member 1's arrest in Nashville.

23. In the above post, BLOYED directs individuals to "harass the owner" of a business establishment in Nashville.

24. In the post below, BLOYED reveals what he believed to be the home address of the victim of the alleged assault committed by GDL member 1.



25. On November 4, 2023, Waxahachie (TX) Police Department officers encountered David Aaron BLOYED as he attempted to distribute GDL flyers outside the Waxahachie Convention Center. Later that day, BLOYED used his Gab account to make the following post:

> I just got ran out of the outside sidewalk entrance to the Waxahachie Texas convention center, I was outside the whole time, I never went inside, and still I got ran off by three ZOG bots telling me "you are detained, and if you do not leave you are under arrest for trespassing" and we will take your firearm and take you to jail. For handing out political/religious flyers on a city owned event center outside sidewalk at a gun show where everyone is armed. I got it all on my body cam and their body cams were on also. So I left and I drove straight to the Police station and dropped off a copy of the "Flyering case law" to the police chief and a few flyers and then I went to the town square/County court house and flyered every car in that Square for Waxahachie/Ellis county and for blocks around it. Fuck you Waxahachie and Ellis county! The 3 stooge Waxahachie City cops are listed below. We have two choices in how to deal with these clowns in the near future: Retraining or Rope. I would let two of them go for "retraining", the other (Lieutenant Young) goes 1/2 way on the Turner rope list and gets one more shot at being worth saving.
>
> Time about 10:30 -11:00 PM 11/4/23

PD non emergency line: 469-309-XXXX

Officers were:

Sargent X. Xxxx - Retraining.

Xxxxx Xxxxx, Lieutenant - Half way to the rope (you've got one more chance nigger)

The younger officer, (I'm still getting his name) - retraining.

26. The FBI contacted the Waxahachie Police Department who confirmed that the individual they encountered above was in fact David Aaron BLOYED.

27. On or about August 26, 2024, Special Agents from FBI Dallas conducted physical surveillance at the 4206 FM 667, Frost, Texas address and observed a Chevy Suburban in the driveway. The current registered owner of that vehicle was Walter BLOYED. Law enforcement database searches revealed Walter BLOYED is David BLOYED's 85-year-old father. According to the Navarro County Property Assessor's Office, 4210 FM 667, Frost, Texas, is property owned by Walter BLOYED, and the 4206 address is occupied by David BLOYED, and is a structure located on the 4210 property. According to the National Crime Information Center (NCIC), David BLOYED is registered as living at the 4206, FM 667, Frost, Texas, address. Physical surveillance conducted at the 4206 FM 667, Frost, Texas, address revealed a wooden post in front of the property that displayed both the 4210 and 4206 addresses (See photographs in Attachment A).

28. On September 6, 2024, law enforcement obtained a ping warrant for the phone connected to BLOYED, 972-567-6523, to determine the precise location of BLOYED on the property described in the preceding paragraph. This warrant revealed that BLOYED's phone is regularly located in the area described in Attachment A.

29. On September 13, 2024, a magistrate judge in the Middle District of Tennessee signed a criminal complaint that charged David Aaron BLOYED with communicating a threat in interstate commerce in violation of Title 18, United States Code, Section 875(c).

30. On September 19, 2024, a Texas law enforcement officer encountered BLOYED, checked his identifiers in a law enforcement database, determined he had a federal arrest warrant, and arrested BLOYED. Following BLOYED's arrest, the ping warrant showed that the cell phone associated with BLOYED, 972-567-6523, remained active at the property described in Attachment A.

TECHNICAL TERMS

26. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

1) A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

2) "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes

electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

3) "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

b. "Wireless telephone" (or mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through "wi-fi" networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional "land line" telephones, computers, and other digital devices. A wireless telephone usually contains a "call log," which records the

telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; utilizing global positioning system ("GPS") locating and tracking technology, and accessing and downloading information from the Internet.

c. A "tablet" is a mobile computer, typically larger than a wireless phone yet smaller than a notebook, that is primarily operated by touch-screen. Like wireless phones, tablets function as wireless communication devices and can be used to access the Internet or other wired or wireless devices through cellular networks, "wi-fi" networks, or otherwise. Tablets typically contain programs called applications ("apps"), which, like programs on both wireless phones, as described above, and personal computers, perform many different functions and save data associated with those functions.

d. A "GPS" navigation device, including certain wireless phones and tablets, uses the Global Positioning System (generally abbreviated "GPS") to display its current location, and often retains records of its historical locations. Some GPS navigation devices can give a user driving or walking directions to another location, and may contain records of the addresses or locations involved in such historical navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly

available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

f. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. Internet Protocol ("IP") Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. The "Internet" is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, fiber-optic, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name, a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

j. A "modem" translates signals for physical transmission to and from the ISP, which then sends and receives the information to and from other computers connected to the Internet.

k. A "router" often serves as a wireless Internet access point for a single or multiple devices, and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant

client inbound traffic arriving from the Internet. A router usually retains logs for any devices using that router for Internet connectivity. Routers, in turn, are typically connected to a modem.

l. "Domain Name" means the common, easy-to-remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

n. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to share files on a computer with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred

between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network to facilitate faster downloading.

1) When a user wishes to share a file, the user adds the file to shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's hash value is recorded by the P2P software. The hash value is independent of the file name; that is, any change in the name of the file will not change the hash value.

2) Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

o. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

p. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

q. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

COMPUTERS, ELECTRONIC/MAGNETIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for evidence, fruits, contraband, instrumentalities, and information that might be found on the PREMISES, in whatever form they are found. One form in which such items might be found is data stored on one or more digital devices. Such devices are defined above and include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related

communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of digital devices or, potentially, the copying of stored information, all under Rule 41(e)(2)(B). Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that, if digital devices are found on the PREMISES, there is probable cause to believe that the items described in Attachment B will be stored in the Device(s) for at least the following reasons:

a. Individuals who engage in criminal activity, including 26 U.S.C. § 5861(e) (illegal transfer of firearms) use digital devices, like the Device, to access websites to facilitate illegal activity and to communicate with co-conspirators online; to store on digital devices, like the Device(s), documents and records relating to their illegal activity, which can include logs of online chats with co-conspirators; email correspondence; text or other "Short Message Service" ("SMS") messages; contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts and photographs of their criminal activity.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed

via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

28. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices,

I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in any of the Device(s) at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the Device(s), not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this

data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs,

anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

29. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive,

are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices, including tablets, can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as "AES-256 encryption" to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, "Hide It Pro," disguises itself as an audio

application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

30. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises.

a. Therefore, in searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

1. Upon securing the PREMISES, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any digital devices (that is, the Device(s)), within the scope of this warrant as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such digital devices at the PREMISES. The digital devices, and/or any digital images

thereof created by law enforcement sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

2. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized digital devices will be specifically chosen to identify the specific items to be seized under this warrant.

BIOMETRIC ACCESS TO DEVICE(S)

31. This warrant permits law enforcement agents to obtain from the person of David Aaron BLOYED (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s). The grounds for this request are as follows:

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

37. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices, the Device(s), will be found during the search. The passcode or password that would unlock the Device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

39. Due to the foregoing, if law enforcement personnel encounter any Device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Device(s), including to

(1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the Device(s) found at the PREMISES; (2) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the Device(s) found at the PREMISES in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the Device(s) in order to search the contents as authorized by this warrant.

40. The proposed warrant does not authorize law enforcement to require that the aforementioned person(s) state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the Device(s). Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

41. Based on the information set forth in this affidavit, I respectfully submit there is probable cause to believe an individual who now resides at 4206 FM667, FROST, NAVARRO COUNTY, TEXAS, the PREMISES, is involved in violations of Title 18, United States Code,

Section 875(c) ("Threatening Interstate Communications"). I respectfully submit that there is probable cause to believe that an individual residing in the residence described above has violated Title 18, United States Code, Section 875(c). Additionally, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 875(c) are presently located at the PREMISES**,** and this evidence, listed in Attachment B, is instrumentalities and evidence which is or has been used as the means of committing the foregoing offenses. Accordingly, I respectfully request that this Court authorize the search of this residence, including any persons at or associated with this residence and any vehicles located at or near the premises that fall under the dominion and control of the persons associated with said premises, so that agents may seize the items listed in Attachment B.

42. Rule 41 of the Federal Rules of Criminal Procedure authorizes the Government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them. I further request that the Court authorize the transfer of any computers, computer storage devices or smartphones to other Government authorized personnel or contractors, within or outside of this District, in the event that advanced expertise is needed to access the files subject to search and seizure under this warrant.

ATTACHMENT A

Property to be searched

The property to be searched is a residence believed to be identified as 4206 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641, including any attached or unattached outbuilding, any persons at or associated with the residence and any vehicles located at or near the premises that fall under the dominion and control of the persons associated with said premises.

The residence believed to be 4206 is described a single-story structure, white in color, a door with steps on the northeast facing side (denoted by the white line in the photograph below). There is a structure with what appears to be a black a roof on the east side (denoted by the green line in the photograph below). It is unknown if the numbers for "4206" are affixed to the structure.

According to Navarro County Property Assessor's Office, 4210 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641 ("4210"), is identified as parcel 39418, and 4206 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641, appears to be on parcel 39417. Both parcels are owned by Walter BLOYED (David Aaron BLOYED's father). The residence believed to be "4206" is not listed on the Navarro County Property Assessor's website as a legal address. An aerial view of the 4210 residence and the residence believed to be 4206 is shown below along with a snippet from the Navarro County Property Assessor's Office for the land parcels. There is one gate that provides access to a road that services both the 4206 and the 4210 residences.

Photograph of Entrance to parcel 4210 FM 667, Frost, Texas and 4206 FM 667

Photographs of the residence believed to be 4206 FM 667, Frost, Texas

ATTACHMENT B

Property to be seized

1. The items to be seized are fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 875(c) and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

   a. Evidence concerning threatening communications;

   b. Evidence concerning any conspiracy, planning, or preparation to commit the above offenses;

   c. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;

   d. Evidence of the state of mind of the subject and/or other co-conspirators, *e.g.*, intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and

   e. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.

2. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:

   a. Any records and/or evidence revealing the Subject's participation in threatening communications;

3. Digital devices used in the commission of, or to facilitate, the above-described offenses.

4. For any digital device which is capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities as described in the search warrant affidavit and above, hereinafter the "Device(s)":

a. evidence of who used, owned, or controlled the Device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

b. evidence of software, or the lack thereof, that would allow others to control the Device(s), such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the attachment to the Device(s) of other storage devices or similar containers for electronic evidence;

d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device(s);

e. evidence of the times the Device(s) was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the Device(s);

g. documentation and manuals that may be necessary to access the Device(s) or to conduct a forensic examination of the Device(s);

h. records of or information about Internet Protocol addresses used by the Device(s); and

i. records of or information about the Device(s)'s Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. During the execution of the search of the PREMISES described in Attachment A, law enforcement personnel are also specifically authorized to obtain from David Aaron BLOYED (but not any other individuals present at the PREMISES at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the Device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the Device(s) found at the PREMISES,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.

6. While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric

characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

7. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Middle District of Tennessee

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

4206 FM667, FROST, NAVARRO COUNTY, TEXAS 76441

Case No. 24-mj-2294

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of Texas *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before October 3, 2024 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Jeffery S. Frensley, U.S. Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of __________.

Date and time issued: September 20, 2024 at 8:00 a.m.

Judge's signature

City and state: Nashville, Tennessee

Jeffery S. Frensley, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is a residence believed to be identified as 4206 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641, including any attached or unattached outbuilding, any persons at or associated with the residence and any vehicles located at or near the premises that fall under the dominion and control of the persons associated with said premises.

The residence believed to be 4206 is described a single-story structure, white in color, a door with steps on the northeast facing side (denoted by the white line in the photograph below). There is a structure with what appears to be a black a roof on the east side (denoted by the green line in the photograph below). It is unknown if the numbers for "4206" are affixed to the structure.

According to Navarro County Property Assessor's Office, 4210 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641 ("4210"), is identified as parcel 39418, and 4206 FM 667, FROST, NAVARRO COUNTY, TEXAS 76641, appears to be on parcel 39417. Both parcels are owned by Walter BLOYED (David Aaron BLOYED's father). The residence believed to be "4206" is not listed on the Navarro County Property Assessor's website as a legal address. An aerial view of the 4210 residence and the residence believed to be 4206 is shown below along with a snippet from the Navarro County Property Assessor's Office for the land parcels. There is one gate that provides access to a road that services both the 4206 and the 4210 residences.

characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the Device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any Device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any Device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

7. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.